Susan S.Q. Kalra (CA State Bar No. 169740)
Email: skalra@rameyfirm.com
RAMEY LLP
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
Telephone: (800) 993-7499
Fax: (832) 900-4941

William P. Ramey, III (*pro hac vice anticipated*)
Texas Bar No. 24027643
RAMEY LLP
Email: wramey@rameyfirm.com
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
(713) 426-3923 (telephone)
(832) 900-4941 (fax)

Attorneys for Plaintiff
STREET SPIRIT IP LLC

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

STREET SPIRIT IP LLC,
Plaintiff,

v.

META PLATFORMS, INC. AND FACEBOOK, INC.
Defendant.

Case No.: 3:23-CV-00879-WHA

OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

DEMAND FOR JURY TRIAL

Hearing date: July 13, 2023
Time: 8:00 a.m.
Courtroom 12
Hon. William H. Alsup

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

OPPOSITION TO MOTION TO DISMISS

Street Spirit IP LLC ("Plaintiff" or "Street Spirit") files this Response to Defendants Meta Platforms, Inc. and Facebook, Inc.'s ("Defendant") Motion Pursuant To Rules 8 And 12(B)(6) Of The Federal Rules Of Civil Procedure ("Defendant's Motion")[1] showing the Court that it should be denied.[2]

I. RELEVANT FACTUAL BACKGROUND AND INTRODUCTION

On March 8, 2016, U.S. Patent No. 9,282,090 ("the '090 patent") entitled "Methods and systems for identity verification in a social network using ratings" was duly and legally issued by the U.S. Patent and Trademark Office. Street Spirit owns the '090 patent by assignment. The '090 patent relates to novel and improved identity verification and management for a social network system. [3] The invention of the '090 patent addresses the problem of providing security against Internet-centric crimes including cyberstalking and cyber-bullying.[4] The claims of the '090 patent do not merely recite the performance of some business practice known from the pre-Internet world along with the requirements to perform it on the Internet. Instead, the solution provided by the '090 patent is rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks. *DDR Holdings, LLC v Hotels.com et al*. 113 USPQ.2d 1097 (Fed. Cir. 2014). Claim 19,[5] for example, recites:

> A method of providing security against cybercrimes using an identification-secured network, the identification-secured network configured to provide security against Internet-related crimes including cyberstalking and cyber-bullying, the method comprising:

---

[1] Doc. No. 17
[2] A motion nearly identical to Defendant's Motion has been filed in Street Spirit IP LLC v Meta Platforms, Inc. and Instagram, No. 5:23-cv-00883-NC (N.D. Cal. Feb. 27, 2023).
[3] See Doc. No. 1-1 (U.S. Patent No. 9,282,090) at Abstract and at column 2, Lines 8-11 (1:8-11).
[4] *Id*. at 2:1-3.
[5] Claim 19 is not representative of all claims as there are multiple independent claims each including relevant features that are not shared in all independent claims.

providing an identity management server connected to a data network, the identity management server including one or more processors, wherein the identity management server is configured to receive, authenticate, and manage requests for access from multiple end user access devices;

creating, via the one or more processors, member account profiles for members of the identification-secured network using identification components for identifying members;

generating, via the one or more processors, an identity rating for each member of the identification-secured network using initial rating factors including: a number of identification components and a quality of identification components;

determining, via the one or more processors, member identity rating thresholds for identity rating-restricted services;

updating, via the one or more processors, the member's identity rating in real-time during an active session, wherein the member's identity rating is alterable in real-time during the active session by monitoring member identity rating-altering factors, and comparing current behavior characteristics against previously recorded behavior characteristics; and

restricting, via the one or more processors, a member's ability to communicate with another member, access content of another member, or both, based at least in part on the member's initial or altered identity rating and identity rating access thresholds of another member.[6]

II. LEGAL STANDARD

A. MOTION TO DISMISS UNDER FED. R. CIV. P. 12(B)(6)

Federal Rule of Civil Procedure 12(b)(6) authorizes a court to dismiss a complaint if the complaint "fail[s] to state a claim upon which relief can be granted." The question resolved on a motion to dismiss for a failure to state a claim is not whether the plaintiff will ultimately prevail, "but whether [the] complaint was sufficient to cross the federal court's threshold." *Skinner v Switzer*, 562 U.S. 521, 530, 131 S.Ct. 1289, 179 L.Ed.2d 233 (2011). When considering a motion to dismiss under Rule 12(b)(6), a court "accept[s] all well-pleaded facts as true, and view[s] those facts in the

[6] Doc. No. 1-1 at 46:65 to 47:32.

light most favorable to the plaintiff." *Bustos v Martini Club, Inc.*, 599 F.3d 458, 461 (5th Cir.2010). (*See, Script Security Solutions, LLC* v *Reebok, Inc.*, 170 F. Supp.3d 928 (E.D. Texas 2016).

"The court's task is to determine whether the plaintiff has stated a legally cognizable claim that is Plausible, not to evaluate the plaintiff's likelihood of success." *Panasonic Corp. v. Magna Int'l., Inc.*, 6:21-cv-00319-ADA, 2022 WL 174513, at *1 (W.D. Tex. Feb 20, 2022) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal quotations omitted). Plaintiff is not required to provide evidence of infringement at the pleading stage beyond "stat[ing] a claim to relief that is plausible on its face." *Id.* "Courts will not dismiss a claim unless the plaintiff 'would not be entitled to relief under any set of facts or any possible theory that it could prove consistent with the allegations in the complaint.'" *Id.* (quoting *Slyce Acquisition, Inc. v. Syte – Visual Conception, Ltd.*, 422 F. Supp. 3d 1191, 1198 (W.D. Tex. 2019)).

"The complaint must be liberally construed in favor of the plaintiff, and all facts pleaded in the complaint must be taken as true." *Collins v. Morgan Stanley Dean Witter*, 224 F.3d 496, 498 (5th Cir. 2000) (quoting *Kaiser Aluminum & Chem. Sales v. Avondale Shipyards*, 677 F.2d 1045, 1050 (5th Cir. 1982)). The "plausibility standard is met when 'the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.'" *Disc Disease Solutions Inc. v. VGH Solutions, Inc.*, 888 F.3d 1256, 1260 (Fed. Cir. 2018) (quoting *Iqbal*, 556 U.S. at 678).

Based upon the assumption that all the allegations in the complaint are true, the factual allegations must be enough to raise a right to relief above the speculative level. *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007). When the nonmovant pleads factual content that allows the court to reasonably infer that the movant is liable for the alleged misconduct, then the claim is plausible on its face. *Ashcroft v. Iqbal*, 556 U.S. 662 at 678 (2009).

B. PATENTABLE SUBJECT MATTER

The Supreme Court articulated a two-step "framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts."[7] At step one, the court must determine whether the claims are directed to one of the three patent-ineligible concepts.[8] If not, "the claims satisfy [Section] 101 and [the court] need not proceed to the second step."[9] If the claims are directed to a patent-ineligible concept, the court must proceed to the second step of identifying an "inventive concept i.e., an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself."[10]

At step one, "the claims are considered in their entirety to ascertain whether their character as a whole is directed to excluded subject matter."[11] However, "courts must be careful to avoid oversimplifying the claims by looking at them generally and failing to account for the specific requirements of the claims."[12]

At step two, the court must "look to both the claim as a whole and the individual claim elements" to determine whether they "amount[ ] to significantly more than a patent upon

---

[7] *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 217, 134 S. Ct. 2347 (2014); *see also Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 77-78, 132 S. Ct. 1289 (2012).

[8] *Alice*, 573 U.S. at 217.

[9] *Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc.*, 880 F.3d 1356, 1361 (Fed. Cir. 2018).

[10] *Alice*, 573 U.S. at 217-18 (quoting *Mayo*, 566 U.S. at 72-73).

[11] *Internet Patents Corp, v. Active Network, Inc.*, 790 F.3d 1343, 1346 (Fed. Cir. 2015); *see also Affinity Labs of Texas, LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016) ("*DIRECTV*") ("The 'abstract idea' step of the inquiry calls upon us to look at the 'focus of the claimed advance over the prior art' to determine if the claim's 'character as a whole' is directed to excluded subject matter.").

[12] *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1313 (Fed. Cir. 2016) (internal quotation marks omitted). "At step one, therefore, it is not enough to merely identify a patent-ineligible concept underlying the claim; [courts] must determine whether that patent-ineligible concept is what the claim is 'directed to." *Rapid Litig. Mgmt. Ltd. v. CellzDirect, Inc.*, 827 F.3d 1042, 1050 (Fed. Cir. 2016).

the ineligible concept itself"[13] "Simply appending conventional steps, specified at a high level of generality, [is] not enough to supply an inventive concept."[14] Instead, the claim elements must involve more than performance of "well-understood, routine, [and] conventional activities previously known to the industry."[15] "The inventive concept inquiry requires more than recognizing that each claim element, by itself, was known in the art. . . . [A]n inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces."[16]

Applying these standards, the claims of the '090 patent are patent eligible.

III. ARGUMENT

A. THE FOCUS OF THE CLAIMED ADVANCE OVER THE PRIOR ART ESTABLISHES THE CLAIMS ARE DIRECTED TO PATENTABLE SUBJECT MATTER.

The focus of the claimed advance over the prior art establishes the claims are directed to patentable subject matter. The '090 patent identifies problems at the time of the invention, namely that social networks at the time of the invention did not utilize sufficiently reliable identify verification systems so that an individual knows with reasonable certainty with whom he or she is communicating. Thus, an identified problem that the '090 patent addresses is a social network user becoming a victim of cyberstalking and/or cyber-bullying.[17]

The claims of the '090 patent are directed to providing security against cybercrimes using an identification-secured network, where the identification-secured network is configured to provide security against Internet-related crimes including cyberstalking and cyber-bullying. The

---

[13] *McRO*, 837 F.3d at 1312.
[14] *Alice*, 573 U.S. at 222
[15] *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1367 (Fed. Cir. 2018) (citation and internal quotation marks omitted); *see also Mayo*, 566 U.S. at 73.
[16] *BASCOM Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1350 (Fed. Cir. 2016).
[17] Doc. No. 1-1 at 1:61-66.

identification-secured network provides (i) an identify management server configured to receive, authenticate, and manage requests for access from multiple end user access devices; (ii) updating a member's identity rating in real-time during an active session, where the member's identity rating is alterable in real-time during an active session by monitoring member identity rating-altering factors, and comparing current behavior characteristics against previously recorded behavior characteristics, and (iii) restricting a member's ability to communicate with another member, access content of another member, or both, based at least in part on the member's initial or altered identity rating and identity rating access thresholds of another member.[18] Thus, the claimed invention, provides a novel method for authenticating a member attempting to access a secured network, updating in *real-time* an identity rating of the member, where the identity rating is alterable in *real-time* and the member's ability to communicate with another member or access content of another member is restricted based on the identity rating and based on an identity rating access thresholds of another member.

The claims address a challenge that is particular to computer software and the Internet (e.g., providing security against Internet-centric crimes including cyberstalking and cyber-bullying).

Furthermore, as noted by the U.S. Patent and Trademark Office (USPTO), these features are novel over the prior art.[19] Street Spirit notes that further discovery is needed to verify the USPTO finding that the prior art does not include the claimed novel method for authenticating a member attempting to access a secured network, updating in *real-time* an identity rating of the member, where the identity rating is alterable in *real-time* and the member's ability to communicate with

[18] See Claim 19 of the '090 patent, Doc. No. 1-1 at 46:65 to 47:32.
[19] See Exhibit A – Notice of Allowability at page 2 noting that the claims are allowable for the reasons provided by applicant's arguments submitted with its Response to Office Action at page 20 of the Response to Office Action.

another member or access content of another member is restricted based on the identity rating and based on an identity rating access thresholds of another member.

B. THE CLAIMS OF THE '368 PATENT ARE DIRECTED TO CONCRETE STEPS

To properly evaluate whether asserted claims "are directed to a patent-eligible concept,"[20] a court must examine "the focus of the claimed advance over the prior art to determine if the character of the claim as a whole, considered in light of the specification, is directed to excluded subject matter."[21] In other words, abstractness is determined by analyzing the claim as a whole, not whether each element standing alone is abstract.[22] Taking the claim as a whole, the focus of the claims is authenticating a member attempting to access a secured network, updating in *real-time* an identity rating of the member, where the identity rating is alterable in *real-time* and the member's ability to communicate with another member or access content of another member is restricted based on the identity rating and based on an identity rating access thresholds of another member ("Focus"). This Focus is support by the Abstract of the '090 patent:

> The disclosed embodiment relates to identity verification and identity management, and in particular, to methods and systems for identifying individuals, identifying users accessing one or more services over a network, determining member identity ratings, and based on member identity ratings that restrict access to identity rating-restricted services and certain user-to-user interactions. Further, the user experience in performing identity management is simplified and enhanced as disclosed herein.[23]

The Focus is also supported by the Detailed Description of the Specification.

---

[20] *Alice Corp. Pty. Ltd.*, 573 U.S. at 218.
[21] *Trading Techs. Int'l, Inc. v. IBG LLC*, 921 F.3d 1084, 1092 (Fed. Cir. 2019).
[22] *See e.g., Alice Corp.*, 574 U.S. 208, 219, 134 S. Ct. 2347, 2359 (2014); *Eyetalk365, LLC v. Zmodo Tech. Corp.*, 356 F. Supp. 3d 1059, 1067 (D. Nev. 2018).
[23] Doc. No. 1-1 at Abstract.

> In another embodiment, the identity verification and management method enables a service provider to offer identity verification services including: creating member account profiles for members using identification components for identifying members; generating an identity rating for each member using initial rating factors including: a number of identification components and a quality of identification components; determining member identity rating thresholds for identity rating-restricted services access; authenticating a member attempting to access the network; managing the member's identity rating in real-time, wherein the member's identity rating is alterable by monitoring member identity rating-altering factors including keystroke patterns and language analysis; and providing identity rating-restricted services access to a member based on the managed identity ratings. [24]

Assessing the focus of the claims from the Specification is proper. The inquiry may also involve looking to the abstract to understand the problem facing the inventor and, ultimately, what the patent describes as the invention.[25] Further support for this Focus is provided in the independent claims. For example, claim 19 recites:

> A method of providing security against cybercrimes using an identification-secured network, the identification-secured network configured to provide security against Internet-related crimes including cyberstalking and cyber-bullying, the method comprising:
>
> providing an identity management server connected to a data network, the identity management server including one or more processors, wherein the identity management server is configured to receive, authenticate, and manage requests for access from multiple end user access devices;
>
> creating, via the one or more processors, member account profiles for members of the identification-secured network using identification components for identifying members;
>
> generating, via the one or more processors, an identity rating for each member of the identification-secured network using initial rating factors including: a number

[24] *Id.* at 2:49-64.

[25] *See ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 767 (Fed. Cir. 2019) *citing TLI Communs. LLC v. AV Auto., L.L.C. (In re TLI Communs. LLC Patent Litig.)*, 823 F.3d 607, 612 (Fed. Cir. 2016); *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371, 1376 (Fed. Cir. 2015) (in the step one analysis, pointing to statements from the specification that supported the identified focus was the key discovery described in the patent).

> of identification components and a quality of identification components;
>
> determining, via the one or more processors, member identity rating thresholds for identity rating-restricted services;
>
> updating, via the one or more processors, the member's identity rating in real-time during an active session, wherein the member's identity rating is alterable in real-time during the active session by monitoring member identity rating-altering factors, and comparing current behavior characteristics against previously recorded behavior characteristics; and
>
> restricting, via the one or more processors, a member's ability to communicate with another member, access content of another member, or both, based at least in part on the member's initial or altered identity rating and identity rating access thresholds of another member.[26]

Claim 19 is directed to providing security against cybercrimes using an identification-secured network, where the identification-secured network is configured to provide security against Internet-related crimes including cyberstalking and cyber-bullying. The identification-secured network provides (i) an identify management server configured to receive, authenticate, and manage requests for access from multiple end user access devices; (ii) updating a member's identity rating in real-time during an active session, where the member's identity rating is alterable in real-time during an active session by monitoring member identity rating-altering factors, and comparing current behavior characteristics against previously recorded behavior characteristics, and (iii) restricting a member's ability to communicate with another member, access content of another member, or both, based at least in part on the member's initial or altered identity rating and identity rating access thresholds of another member.[27] Thus, the claimed invention, provides a novel method for authenticating a member attempting to access a secured network, updating in *real-time* an identity rating of the member, where the identity rating is alterable in *real-time* and

[26] Doc. No. 1-1 at 46:65 to 47:32.
[27] See Claim 19 of the '090 patent, Doc. No. 1-1 at 46:65 to 47:32.

the member's ability to communicate with another member or access content of another member is restricted based on the identity rating and based on an identity rating access thresholds of another member.

The '090 patent specification provides substantial detail for the claimed invention and its interconnectivity with each claimed element for sufficient specificity to be concrete.[28] For instance, the '090 patent provides reference to systems and methods through the detailed diagrams and flowcharts that can be used to perform the solutions of the claimed inventions; FIG. 1 illustrates a network operating environment for an Identity Management ("IDM") system; FIG. 2 illustrates an IDM administration user interface menu selection screen; FIG. 3 illustrates an IDM administration user interface login screen; FIG. 4 illustrates an IDM administration user interface new user account creation screen; FIG. 5 illustrates an IDM administration user interface temporary user name and password assignment screen; FIG. 6 illustrates an IDM administration user interface photograph upload confirmation screen; FIG. 7 illustrates an IDM administration user interface, new user, biometric capture selection screen; FIG. 8 illustrates an IDM administration user interface iris scan instruction screen; FIG. 9 illustrates an IDM administration user interface iris scan upload confirmation screen; FIG. 10 illustrates an IDM administration user interface security questions selection screen; FIG. 11 illustrates an IDM administration user interface identity credentials verification screen; FIG. 12 illustrates an IDM administration user interface initial and threshold identity rating display; FIG. 13 illustrates a smartphone user interface with the IDM system application icon, "Verify;" FIG. 14 illustrates a smartphone application display requesting user name and password entry; FIG. 15 illustrates a smartphone application display depicting the display of a security question; FIG. 16 illustrates a smartphone

[28] *See, e.g., SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1167 (Fed. Cir. 2018).

application display depicting a user selection of an answer to a security question; FIG. 17 illustrates a smartphone application display depicting a display requesting the user to reset their temporary user name and password; FIG. 18 illustrates an IDM user interface user login screen; FIG. 19 illustrates an IDM user interface depicting a menu of means for enhancing a user's session identity rating; FIG. 20 illustrates an IDM user interface depicting user instructions for capturing an iris scan; FIG. 21 illustrates a smartphone application depicting a menu of biometric identity verification options; FIG. 22 illustrates a smartphone IDM application display in iris scan image capture mode; FIG. 23 illustrates an IDM user interface depicting a display requesting the user to answer a security question; FIG. 24 illustrates an IDM user interface depicting a display requesting the user to reset their temporary user name and password; FIG. 25 illustrates an IDM user interface depicting a parent/guardian dashboard display; FIG. 26 illustrates an IDM user interface depicting a tabular display of a user's transaction history; FIG. 27 illustrates an IDM user interface depicting a display of a user's previous chat session; FIG. 28 illustrates an IDM user interface depicting user instructions for capturing a fingerprint scan; FIG. 29 illustrates an IDM user interface depicting a dating site user home page; FIG. 30 illustrates an IDM user interface depicting a dating site user home page with a system terminated chat session; FIGS. 31-37 illustrate the operating environment/process workflow of a first embodiment of a social network member scenario; FIGS. 38-40 illustrate the operating environment/process workflow of a second embodiment of an on-line dating scenario.

In short, there is ample disclosure of how to implement embodiments of the claimed invention.

C. DEFENDANT OVERSIMPLIFIES THE CLAIMED INVENTION AND IGNORES IMPORTANT LIMITATIONS.

Defendant's Motion is an oversimplification and focuses on claim elements rather than the

claim as a whole. Defendant "describe[s] the claims at such a high level of abstraction and untethered from the language of the claims that all but ensures that the exceptions to §101 swallow the rule."[29] For instance, Defendant's Motion over generalizes the teachings of the patent by providing that "claim 19… is directed to the abstract idea of controlling an individual's access to certain resources."[30]

Defendant's description of Plaintiff's claimed invention fails to specifically mention the claim features of the identification-secured network (i) providing an identify management server …configured to receive, authenticate, and manage requests for access from multiple end user access devices; (ii) updating… the member's identity rating in real-time during an active session, where the member's identity rating is alterable in real-time during an active session by monitoring member identity rating-altering factors, and comparing current behavior characteristics against previously recorded behavior characteristics, and (iii) restricting a member's ability to communicate with another member, access content of another member, or both, based at least in part on the member's initial or altered identity rating and identity rating access thresholds of another member.[31]

These are claim features that were identified by the USPTO Examiner as being novel in view of the prior art.[32]

The Defendant's Motion further characterizes the claims as a common place human concept, arguing that humans have long relied on varying degrees of identification to provide access to certain resources.[33] This again is an oversimplification. The claimed features address a

---

[29] *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1337 (Fed. Cir. 2016).
[30] See Doc. No. 17 at page 15.
[31] See Claim 19 of the '090 patent, Doc. No. 1-1 at 46:65 to 47:32.
[32] See Exhibit A – Notice of Allowability at page 2 noting that the claims are allowable for the reasons provided by applicant's arguments submitted with its Response to Office Action at page 20 of the Response to Office Action.
[33] Doc. No. 18 at 16.

challenge that is particular to computer software and the Internet (e.g., providing security against Internet-centric crimes including cyberstalking and cyber-bullying). The claimed invention differs from other claims found by the courts to recite abstract ideas in that it does not "merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet. Instead, the claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks." *DDR Holdings, LLC v. Hotels.com et al.*, 113 USPQ.2d 1097 (Fed.Cir.2014). The invention claimed here is directed towards specially constructed physical devices that provide a technological improvement to an identification-secured network that is configured to providing security against Internet-centric crimes including cyberstalking and cyber-bullying, a concept inextricably tied to computer technology.

D. DEFENDANT'S CASELAW IS NOT APPLICABLE

The Defendant's Motion relies on *PersonalWeb techs. LLC v. Google LLC*, 8 F.4th 1310, 1316 (Fed. Cir. 2021) when arguing that the claimed activities are akin to--and depend on—activities that can be performed in the human mind.[34] However, the claimed features can not practically be performed in the human mind or by taking pen to paper. For example, "updating, via the one or more processors, the member's identity ***rating in real-time*** during an active session, wherein the member's identity rating is ***alterable in real-time*** during the active session by monitoring member identity rating-altering factors, and comparing current behavior characteristics against previously recorded behavior characteristics," as recited in claim 19 of the '090 patent, cannot practically be performed in the human mind.

Defendant's Motion also relies on *Ericsson Inc. v. TCL Commc'n Tech. Holdings* , 955 F.3d

[34] Doc. No. 17 at 16.

1317 (Fed. Cir. 2020) and on *Prism Techs. LLC v. T-Mobile USA, Inc*., 696 F. App'x 1014, 1017 (Fed. Cir. 2017) when asserting that claim 19 recites the type of resource access control activities that the Federal Circuit has found abstract.[35] However, again, Defendant's oversimplify the claims. The claimed features cannot be practically performed by a human mind. Instead, the claims as a whole do provide for an improvement in how the computer system itself operates. The claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks. See *DDR Holdings, LLC v Hotels.com* et al,, 113 USPQ.2d 1097 (Fed. Cir. 2014). More specifically, the claims are directed towards specially constructed physical devices that provide a technological improvement of an identification-secured network that is configured to providing security against Internet-centric crimes including cyberstalking and cyber-bullying, a concept inextricably tied to computer technology and distinct from the types of concepts found by the courts to be abstract.

The Defendant cites *Enfish, LLC v. Microsoft Corp*., 822 F.3d 1327, 1336 (Fed. Cir. 2016) (improved database technology) when asserting that the claimed invention allegedly is not like the type of specific improvements in computer capabilities, particular solutions to computer-specific problems, that the Federal Circuit has found eligible.[36] On the contrary, as previously noted the claimed solution is necessarily rooted in computer technology to overcome a problem specifically arising in the realm of computer networks, namely, providing a technological improvement to an identification-secured network that is configured to providing security against Internet-centric crimes including cyberstalking and cyber-bullying, which is inextricably tied to computer technology.

[35] *Id.* at 11.
[36] *Id*. at 19.

E. THERE ARE INVENTIVE ASPECTS OF THE '090 PATENT THAT PRECLUDE DISMISSAL AT THIS STAGE

While a court may determine patent eligibility at the Rule 12(b)(6) stage, it is "only when there are no factual allegations that, taken as true, prevent resolving the eligibility question as a matter of law."[37] "Plausible factual allegations may preclude dismissing a case under § 101."[38] Here, Plaintiff makes numerous factual allegations in the specification that are not rebutted.

Even if this Court determines Plaintiff's claims are directed towards an abstract idea, patent eligibility is possible if the abstract idea include[s] 'additional features' to ensure that the claim is more than a drafting effort designed to monopolize the abstract idea."[39] "These additional features cannot simply be well-understood, routine, conventional activities previously known to the industry."[40] The primary improvement over the prior art mentioned in the patent specification is a claimed improvement, namely, the use of identification-secured network that is configured to provide security against Internet-centric crimes including cyberstalking and cyber-bullying. Claim 19 provides for an improvement over the prior art at the time of the invention. There are factual allegations of improvements over the prior art, which must be taken as true at this stage of the litigation.[41]

The '090 patent's specification teaches the claimed improvements was not available prior to

---

[37] *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1125 (Fed. Cir. 2018).
[38] *Id.*
[39] *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 773 (Fed. Cir. 2019) (quotations and alterations omitted); *see also Trading Techs.*, 921 F.3d at 1093 ("Step two 'looks more precisely at what the claim elements add' to determine if 'they identify an inventive concept in the application of the ineligible matter to which...the claim is directed." (quoting *SAP*, 898 F.3d at 1167).
[40] *ChargePoint*, 920 F.3d at 773 (quotation and alteration omitted); *see HP Inc.*, 881 F.3d at 1367 ("The second step of the *Alice* test is satisfied when the claim limitations involve more than performance of well-understood, routine, and conventional activities previously known to the industry." (quotation and alteration omitted)
[41] *Aatrix Software, Inc.*, 882 F.3d at 1125; *Guidry v. Am. Pub. Life Ins. Co*, 512 F.3d 177, 180 (5th Cir. 2007).

the invention of the claims of the '090 patent. Thus, taking all inferences in Plaintiff's favor,[42] dismissal at this stage is inappropriate.[43]

IV. CONCLUSION

Plaintiff respectfully requests and prays that the Court deny, in its entirety, Defendant's Motion to Dismiss.

Dated: June 21, 2023

Respectfully submitted,

RAMEY LLP

/s/ Susan S.Q. Kalra
Susan S.Q. Kalra (CA State Bar No. 16740)
Email: skalra@rameyfirm.com
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
Telephone: (800) 993-7499
Fax: (832) 900-4941

/s/ William P. Ramey, III
William P. Ramey, III (*pro hac vice* anticipated)
Texas Bar No. 24027643
Email: wramey@rameyfirm.com
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
Telephone: (713) 426-3923
Fax: (832) 689-9175

Attorneys for Plaintiff
STREET SPIRIT IP LLC

[42] *Guidry*, 512 F.3d at 180.
[43] *Aatrix Software, Inc.*, 882 F.3d AT 1125; *see also Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018).